

INFORMATION PROCESSOR, INFORMATION PROCESSING METHOD, INFORMATION RECORDING MEDIUM AND PROGRAM PROVIDING MEDIUM

Publication number: JP2001351322

Publication date: 2001-12-21

Inventor: ASANO TOMOYUKI; OSAWA YOSHITOMO; NAKANO KATSUHIKO; KITAJIMA MARIKO

Applicant: SONY CORP

Classification:

- international: G06F12/14; G06F21/24; G06Q50/00; G11B20/10;
G06F12/14; G06F21/00; G06Q50/00; G11B20/10;
(IPC1-7): G11B20/10; G06F12/14; G06F17/60

- European:

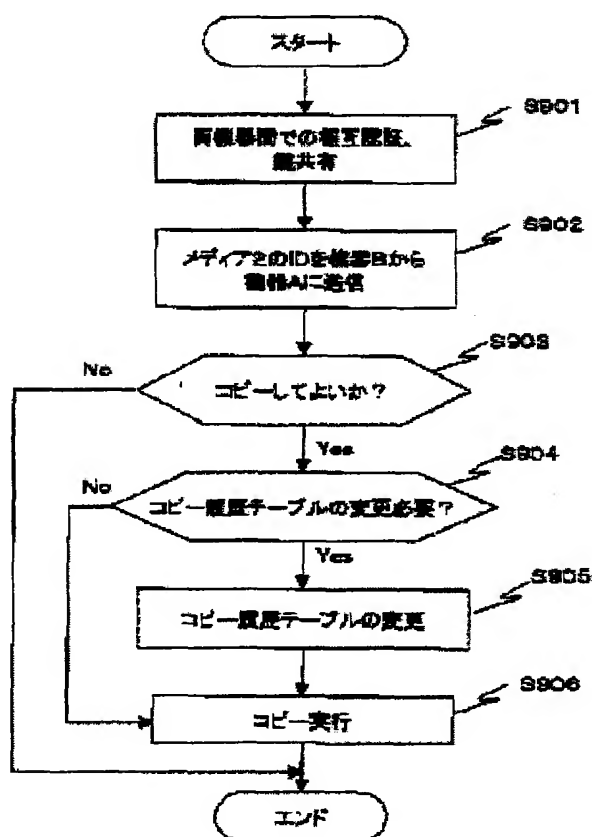
Application number: JP20000170603 20000607

Priority number(s): JP20000170603 20000607

Report a data error here

Abstract of JP2001351322

PROBLEM TO BE SOLVED: To provide an information processor and an information processing method which can limit the number of copies. **SOLUTION:** This constitution includes a copy history table where the number of allowable copies is set in response to the contents data in addition to the contents. The copy history table is prepared for every content data. On the basis of the tables, it is decided whether or not the copy processing should be carried out. Then the copy processing is inhibited after number of copies reaches the upper limit. The IDs of media which carry out the copy processing are written in a copy storage destination media ID column set in response to the contents IDs in the copy history tables before the copy processing carried out to another device. When the number of copies exceeds the number set as the copy numbers of the copy history tables, the media IDs are not written and the copy processing is not permitted.



Data supplied from the esp@cenet database - Worldwide

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2001-351322

(P2001-351322A)

(43) 公開日 平成13年12月21日 (2001. 12. 21)

(51) Int.Cl. ⁷	識別記号	F I	テーマコード(参考)
G 1 1 B 20/10		G 1 1 B 20/10	H 5 B 0 1 7 D 5 B 0 4 9 F 5 D 0 4 4
G 0 6 F 12/14	3 2 0	G 0 6 F 12/14	3 2 0 E 3 2 0 F
審査請求 未請求 請求項の数25 O L (全 25 頁) 最終頁に続く			

(21) 出願番号 特願2000-170603(P2000-170603)

(22) 出願日 平成12年6月7日(2000. 6. 7)

特許法第64条第2項ただし書の規定により×印の部分は
不掲載とした。

(71) 出願人 000002185

ソニー株式会社

東京都品川区北品川6丁目7番35号

(72) 発明者 浅野 智之

東京都品川区北品川6丁目7番35号 ソニ
ー株式会社内

(72) 発明者 大澤 義知

東京都品川区北品川6丁目7番35号 ソニ
ー株式会社内

(74) 代理人 100101801

弁理士 山田 英治 (外2名)

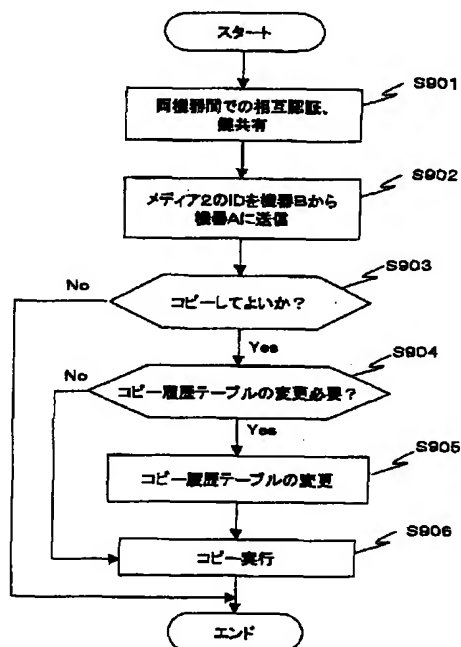
最終頁に続く

(54) 【発明の名称】 情報処理装置、情報処理方法、および情報記録媒体、並びにプログラム提供媒体

(57) 【要約】

【課題】 コピーの数を制限することを可能とした情報
処理装置および情報処理方法を提供する。

【解決手段】 コンテンツデータに対応して許容可能な
コピー数を設定したコピー履歴テーブルをコンテンツと
ともに保有する構成とした。コンテンツデータごとにコ
ピーの履歴テーブルを作成し、それに基づいてコピーを
行うかどうか判定し、上限に達した以降のコピー処理を
不可とする。他デバイスに対するコピー実行の前に、コ
ピー履歴テーブル中のコンテンツIDに対応して設定さ
れたコピー格納先メディアID欄に、コピーを実行する
メディアのメディアIDを書き込む処理を実行する構成
とし、コピー履歴テーブルのコピー番号として設定され
た数を超える場合は、メディアIDの書き込みが実行さ
れずコピーを不許可とする。



【特許請求の範囲】

【請求項 1】コンテンツデータを格納したコンテンツ格納記録媒体からコンテンツデータを他の情報処理装置または他の記録媒体に出力可能な情報処理装置において、前記コンテンツ格納記録媒体に格納されたコンテンツデータについての、前記他の情報処理装置または他の記録媒体に対するコピー可否判定処理を、前記コンテンツデータ毎のコピー可能回数を設定したコピー履歴テーブルに基づいて判定する制御手段を有することを特徴とする情報処理装置。

【請求項 2】前記コピー履歴テーブルには、コピー可能回数に対応して設定されるコピー番号と、コピー番号毎に対応して設定されるコピー格納先メディア ID 設定欄を有し、

前記制御手段は、コンテンツデータのコピー先となる他の情報処理装置または他の記録媒体の識別子を前記コピー格納先メディア ID 欄に記録したことを条件として前記コンテンツ格納記録媒体からのコピーを実行する構成を有することを特徴とする請求項 1 に記載の情報処理装置。

【請求項 3】前記コピー履歴テーブルは、前記コンテンツ格納記録媒体、または該コンテンツ格納記録媒体を装着した情報処理装置内のメモリに暗号化されたデータとして格納された構成であることを特徴とする請求項 1 に記載の情報処理装置。

【請求項 4】前記コピー履歴テーブルの暗号化キーは、前記コンテンツ格納記録媒体の識別子と、前記情報処理装置に格納されたマスターキーとに基づいて生成される暗号化キーであることを特徴とする請求項 3 に記載の情報処理装置。

【請求項 5】前記コピー履歴テーブルには、コピー可能回数に対応して設定されるコピー番号と、コピー番号毎に対応して設定されるコピー格納先メディア ID 設定欄を有し、

前記制御手段は、コンテンツデータのコピー先となる他の情報処理装置または他の記録媒体の識別子と同一の識別子が既に前記コピー格納先メディア ID 欄に記録されている場合には、同一の識別子を有する他の情報処理装置または他の記録媒体に対する前記コンテンツ格納記録媒体からのコピーを実行する構成を有することを特徴とする請求項 1 に記載の情報処理装置。

【請求項 6】前記コピー履歴テーブルには、複数のコンテンツデータの各々に対応して許容可能な個別のコピー可能回数が設定された構成であることを特徴とする請求項 1 に記載の情報処理装置。

【請求項 7】前記情報処理装置は、さらに、コピーの可否を設定したコピー制御情報に基づいて、前記コンテンツデータを格納したコンテンツ格納記録媒体からのコンテンツデータのコピーの可否を判定する構成

を有し、

前記コピー制御情報には、コピーの可否とともに、コピーの許容回数が設定されていることを示す態様としての、コピー数制限ありを示す情報を含み、

前記制御手段は、

前記コピー制御情報がコピー数制限ありを示す情報であるか否かを判定し、コピー数制限ありを示すコピー制御情報であると判定されたことを条件として、前記他の情報処理装置または他の記録媒体に対するコピー可否判定処理を、前記コンテンツデータ毎のコピー可能回数を設定したコピー履歴テーブルに基づいて実行する構成を有することを特徴とする請求項 1 に記載の情報処理装置。

【請求項 8】前記情報処理装置は、さらに、コンテンツデータの受信に際して、コピーの可否を設定したコピー制御情報を受信し、コピー制御情報が、コピーの許容回数が設定されていることを示す態様としてのコピー数制限ありを示す情報である場合に、前記コピー履歴テーブルを生成して、生成したコピー履歴テーブルに基づくコピー制御処理を実行する構成を有することを特徴とする請求項 1 に記載の情報処理装置。

【請求項 9】前記情報処理装置は、さらに、コンテンツデータの受信に際して、コピーの可否を設定したコピー制御情報を受信し、コピー制御情報が、コピーの許容回数が設定されていることを示す態様としてのコピー数制限ありを示す情報であり、さらにコピーの許容回数の指定データが前記コピー制御情報に含まれる場合に、前記コピー履歴テーブルを、前記コピー制御情報中のコピーの許容回数データに基づいて生成して、生成したコピー履歴テーブルに基づくコピー制御処理を実行する構成を有することを特徴とする請求項 8 に記載の情報処理装置。

【請求項 10】前記情報処理装置は、さらに、コンテンツデータの受信に際して、コピーの可否を設定したコピー制御情報を受信し、コピー制御情報が、コピーの許容回数が設定されていることを示す態様としてのコピー数制限ありを示す情報であり、コピーの許容回数の指定データが前記コピー制御情報に含まれない場合に、前記コピー履歴テーブルを、前記情報処理装置に予め設定済みのコピー許容回数データに基づいて生成して、生成したコピー履歴テーブルに基づくコピー制御処理を実行する構成を有することを特徴とする請求項 8 に記載の情報処理装置。

【請求項 11】前記情報処理装置は、さらに、コンテンツデータの受信に際して、受信コンテンツに対応するコピー履歴テーブルを受信し、受信したコピー履歴テーブルに基づくコピー制御処理を実行する構成を有することを特徴とする請求項 1 に記載の情報処理装置。

【請求項 12】コンテンツデータを格納したコンテンツ格納記録媒体からコンテンツデータを他の情報処理装置または他の記録媒体に出力可能な情報処理装置における

情報処理方法であり、

前記コンテンツ格納記録媒体に格納されたコンテンツデータについての、前記他の情報処理装置または他の記録媒体に対するコピー可否判定処理を、前記コンテンツデータ毎のコピー可能回数を設定したコピー履歴テーブルに基づいて判定することを特徴とする情報処理方法。

【請求項 13】前記コピー履歴テーブルには、コピー可能回数に対応して設定されるコピー番号と、コピー番号毎に対応して設定されるコピー格納先メディア ID 設定欄を有し、

前記コピー可否判定処理は、コンテンツデータのコピー先となる他の情報処理装置または他の記録媒体の識別子を前記コピー格納先メディア ID 欄に記録可能か否かを判定するステップと、前記コピー格納先メディア ID 欄に記録可能であることを条件として前記コンテンツ格納記録媒体からのコピーを可能と判定するステップと、を含むことを特徴とする請求項 12 に記載の情報処理方法。

【請求項 14】前記情報処理方法において、さらに、前記コンテンツ格納記録媒体の識別子と、前記情報処理装置に格納されたマスターキーとに基づいて、暗号化キーを生成し、前記暗号化キーに基づいて前記コピー履歴テーブルを暗号化して前記コンテンツ格納記録媒体、または該コンテンツ格納記録媒体を装着した情報処理装置内のメモリに格納する処理を実行することを特徴とする請求項 12 に記載の情報処理方法。

【請求項 15】前記コピー履歴テーブルには、コピー可能回数に対応して設定されるコピー番号と、コピー番号毎に対応して設定されるコピー格納先メディア ID 設定欄を有し、

前記コピー可否判定処理は、コンテンツデータのコピー先となる他の情報処理装置または他の記録媒体の識別子と同一の識別子が既に前記コピー格納先メディア ID 欄に記録されている場合には、同一の識別子を有する他の情報処理装置または他の記録媒体に対する前記コンテンツ格納記録媒体からのコピーを実行可と判定することを特徴とする請求項 12 に記載の情報処理方法。

【請求項 16】前記情報処理方法において、さらに、コピーの可否を設定したコピー制御情報に基づいて、前記コンテンツデータを格納したコンテンツ格納記録媒体からのコンテンツデータのコピーの可否を判定するステップを有し、

前記コピー制御情報には、コピーの可否とともに、コピーの許容回数が設定されていることを示す態様としての、コピー数制限ありを示す情報を含み、前記コピー制御情報がコピー数制限ありを示す情報であるか否かを判定し、

コピー数制限ありを示すコピー制御情報であると判定されたことを条件として、前記他の情報処理装置または他の記録媒体に対するコピー可否判定処理を、前記コンテンツデータ毎のコピー可能回数を設定したコピー履歴テーブルに基づいて実行することを特徴とする請求項 12 に記載の情報処理方法。

【請求項 17】前記情報処理方法は、さらに、コンテンツデータの受信に際して、コピーの可否を設定したコピー制御情報を受信し、

10 コピー制御情報が、コピーの許容回数が設定されていることを示す態様としてのコピー数制限ありを示す情報である場合に、前記コピー履歴テーブルを生成して、生成したコピー履歴テーブルに基づくコピー制御処理を実行することを特徴とする請求項 12 に記載の情報処理方法。

【請求項 18】前記情報処理方法は、さらに、コンテンツデータの受信に際して、コピーの可否を設定したコピー制御情報を受信し、コピー制御情報が、コピーの許容回数が設定されていることを示す態様としてのコピー数制限ありを示す情報であり、さらにコピーの許容回数の指定データが前記コピー制御情報に含まれる場合に、前記コピー履歴テーブルを、前記コピー制御情報中のコピーの許容回数データに基づいて生成して、生成したコピー履歴テーブルに基づくコピー制御処理を実行することを特徴とする請求項 17 に記載の情報処理方法。

【請求項 19】前記情報処理方法は、さらに、コンテンツデータの受信に際して、コピーの可否を設定したコピー制御情報を受信し、コピー制御情報が、コピーの許容回数が設定されていることを示す態様としてのコピー数制限ありを示す情報であり、コピーの許容回数の指定データが前記コピー制御情報に含まれない場合に、前記コピー履歴テーブルを、前記情報処理装置に予め設定済みのコピー許容回数データに基づいて生成して、生成したコピー履歴テーブルに基づくコピー制御処理を実行することを特徴とする請求項 17 に記載の情報処理方法。

【請求項 20】前記情報処理方法は、さらに、コンテンツデータの受信に際して、受信コンテンツに対応するコピー履歴テーブルを受信し、受信したコピー履歴テーブルに基づくコピー制御処理を実行することを特徴とする請求項 12 に記載の情報処理方法。

【請求項 21】コンテンツデータを格納した情報記録媒体であり、前記記録媒体に格納されたコンテンツデータについて、コンテンツデータ毎のコピー可能回数を設定したコピー履歴テーブルを格納したことを特徴とする情報記録媒体。

【請求項 22】前記コピー履歴テーブルには、コピー可能回数に対応して設定されるコピー番号と、コピー番号

毎に対応して設定されるコピー格納先メディアID設定欄を有することを特徴とする請求項21に記載の情報記録媒体。

【請求項23】前記コピー履歴テーブルは、前記コンテンツ格納記録媒体の識別子と、前記情報処理装置に格納されたマスターキーとに基づいて生成される暗号化キーで暗号化されて格納された構成であることを特徴とする請求項21に記載の情報記録媒体。

【請求項24】前記コピー履歴テーブルには、複数のコンテンツデータの各々に対応して許容可能な個別のコピー可能回数が設定された構成であることを特徴とする請求項21に記載の情報記録媒体。

【請求項25】コンテンツ格納記録媒体に格納されたコンテンツデータについての、他の情報処理装置または他の記録媒体に対するコピー可否判定処理をコンピュータ・システム上で実行せしめるコンピュータ・プログラムを提供するプログラム提供媒体であって、前記コンピュータ・プログラムは、コンテンツデータのコピー先となる他の情報処理装置または他の記録媒体の識別子を前記コピー格納先メディアID欄に記録可能か否かを判定するステップと、前記コピー格納先メディアID欄に記録可能であることを条件として前記コンテンツ格納記録媒体からのコピーが可能であると判定するステップと、を有することを特徴とするプログラム提供媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、情報処理装置、情報処理方法、および情報記録媒体、並びにプログラム提供媒体に関し、特に、データ記録再生可能な記録媒体に対するデータ書き込み、データ再生処理における違法コピーを防止することを可能とした情報処理装置、情報処理方法、および情報記録媒体、並びにプログラム提供媒体に関する。

【0002】

【従来の技術】デジタル信号処理技術の進歩、発展に伴い、近年においては、情報を、デジタル的に記録する記録装置や記録媒体が普及しつつある。このようなデジタル記録装置および記録媒体によれば、例えば画像や音声を劣化させることなく記録、再生を繰り返すことができる。このようにデジタルデータは画質や音質を維持したまま何度もコピーを繰り返し実行することができるため、コピーが違法に行われた記録媒体が市場に流通することになると、音楽、映画等各種コンテンツの著作権者、あるいは正当な販売権者等の利益が害されることになる。昨今では、このようなデジタルデータの不正なコピーを防ぐため、デジタル記録装置および記録媒体に違法なコピーを防止するための様々な仕組み（システム）が導入されている。

【0003】例えば、MD（ミニディスク）（MDは商

標）装置において、違法なコピーを防止する方法として、SCMS（Serial Copy Management System）が採用されている。SCMSは、データ再生側において、オーディオデータとともにSCMS信号をデジタルインタフェース（DIF）から出力し、データ記録側において、再生側からのSCMS信号に基づいて、再生側からのオーディオデータの記録を制御することにより違法なコピーを防止するシステムである。

【0004】具体的にはSCMS信号は、オーディオデータが、何度でもコピーが許容されるコピーフリー（copy free）のデータであるか、1度だけコピーが許されている（copy once allowed）データであるか、またはコピーが禁止されている（copy prohibited）データであるかを表す信号である。データ記録側において、デジタルインタフェース（DIF）からオーディオデータを受信すると、そのオーディオデータとともに送信されるSCMS信号を検出する。そして、SCMS信号が、コピーフリー（copy free）となっている場合には、オーディオデータをSCMS信号とともにミニディスクに記録する。また、SCMS信号が、コピーを1度のみ許可（copy once allowed）となっている場合には、SCMS信号をコピー禁止（copy prohibited）に変更して、オーディオデータとともに、ミニディスクに記録する。さらに、SCMS信号が、コピー禁止（copy prohibited）となっている場合には、オーディオデータの記録を行わない。このようなSCMSを使用した制御を行なうことで、ミニディスク装置では、SCMSによって、著作権を有するオーディオデータが、違法にコピーされるのを防止するようになっている。

【0005】

【発明が解決しようとする課題】しかしながら、上記のSCMSで行えるのは、コピーの世代管理のみである。例えば、コピーを1度のみ許可（copy once allowed）とされるデータは、子から孫を作るコピーが禁じられるのみであり、元データからは複数のコピー（子）を作ることが可能である。今後のネットワーク社会においては、音楽などのコンテンツデータに対し、よりきめ細かくコピーの制御を行いたいという要望が著作権者などから出されている。本発明は、データごとに作られるコピー（子）の数を制限できる情報処理装置、情報処理方法、および情報記録媒体、並びにプログラム提供媒体を提供することを目的とする。

【0006】

【課題を解決するための手段】本発明の第1の側面は、コンテンツデータを格納したコンテンツ格納記録媒体からコンテンツデータを他の情報処理装置または他の記録媒体に出力可能な情報処理装置において、前記コンテンツ格納記録媒体に格納されたコンテンツデータについての、前記他の情報処理装置または他の記録媒体に対するコピー可否判定処理を、前記コンテンツデータ毎のコピ

ー可能回数を設定したコピー履歴テーブルに基づいて判定する制御手段を有することを特徴とする情報処理装置にある。

【0007】さらに、本発明の情報処理装置の一実施態様において、前記コピー履歴テーブルには、コピー可能回数に対応して設定されるコピー番号と、コピー番号毎に対応して設定されるコピー格納先メディアID設定欄を有し、前記制御手段は、コンテンツデータのコピー先となる他の情報処理装置または他の記録媒体の識別子を前記コピー格納先メディアID欄に記録したことを条件として前記コンテンツ格納記録媒体からのコピーを実行する構成を有することを特徴とする。

【0008】さらに、本発明の情報処理装置の一実施態様において、前記コピー履歴テーブルは、前記コンテンツ格納記録媒体、または該コンテンツ格納記録媒体を装着した情報処理装置内のメモリに暗号化されたデータとして格納された構成であることを特徴とする。

【0009】さらに、本発明の情報処理装置の一実施態様において、前記コピー履歴テーブルの暗号化キーは、前記コンテンツ格納記録媒体の識別子と、前記情報処理装置に格納されたマスターキーとに基づいて生成される暗号化キーであることを特徴とする。

【0010】さらに、本発明の情報処理装置の一実施態様において、前記コピー履歴テーブルには、コピー可能回数に対応して設定されるコピー番号と、コピー番号毎に対応して設定されるコピー格納先メディアID設定欄を有し、前記制御手段は、コンテンツデータのコピー先となる他の情報処理装置または他の記録媒体の識別子と同一の識別子が既に前記コピー格納先メディアID欄に記録されている場合には、同一の識別子を有する他の情報処理装置または他の記録媒体に対する前記コンテンツ格納記録媒体からのコピーを実行する構成を有することを特徴とする。

【0011】さらに、本発明の情報処理装置の一実施態様において、前記コピー履歴テーブルには、複数のコンテンツデータの各々に対応して許容可能な個別のコピー可能回数が設定された構成であることを特徴とする。

【0012】さらに、本発明の情報処理装置の一実施態様において、前記情報処理装置は、さらに、コピーの可否を設定したコピー制御情報に基づいて、前記コンテンツデータを格納したコンテンツ格納記録媒体からのコンテンツデータのコピーの可否を判定する構成を有し、前記コピー制御情報には、コピーの可否とともに、コピーの許容回数が設定されていることを示す態様としての、コピー数制限ありを示す情報を含み、前記制御手段は、前記コピー制御情報がコピー数制限ありを示す情報であるか否かを判定し、コピー数制限ありを示すコピー制御情報であると判定されたことを条件として、前記他の情報処理装置または他の記録媒体に対するコピー可否判定処理を、前記コンテンツデータ毎のコピー可能回数を設

定したコピー履歴テーブルに基づいて実行する構成を有することを特徴とする。

【0013】さらに、本発明の情報処理装置の一実施態様において、前記情報処理装置は、さらに、コンテンツデータの受信に際して、コピーの可否を設定したコピー制御情報を受信し、コピー制御情報が、コピーの許容回数が設定されていることを示す態様としてのコピー数制限ありを示す情報である場合に、前記コピー履歴テーブルを生成して、生成したコピー履歴テーブルに基づくコピー制御処理を実行する構成を有することを特徴とする。

【0014】さらに、本発明の情報処理装置の一実施態様において、前記情報処理装置は、さらに、コンテンツデータの受信に際して、コピーの可否を設定したコピー制御情報を受信し、コピー制御情報が、コピーの許容回数が設定されていることを示す態様としてのコピー数制限ありを示す情報であり、さらにコピーの許容回数の指定データが前記コピー制御情報に含まれる場合に、前記コピー履歴テーブルを、前記コピー制御情報中のコピーの許容回数データに基づいて生成して、生成したコピー履歴テーブルに基づくコピー制御処理を実行する構成を有することを特徴とする。

【0015】さらに、本発明の情報処理装置の一実施態様において、前記情報処理装置は、さらに、コンテンツデータの受信に際して、コピーの可否を設定したコピー制御情報を受信し、コピー制御情報が、コピーの許容回数が設定されていることを示す態様としてのコピー数制限ありを示す情報であり、コピーの許容回数の指定データが前記コピー制御情報に含まれない場合に、前記コピー履歴テーブルを、前記情報処理装置に予め設定済みのコピー許容回数データに基づいて生成して、生成したコピー履歴テーブルに基づくコピー制御処理を実行する構成を有することを特徴とする。

【0016】さらに、本発明の情報処理装置の一実施態様において、前記情報処理装置は、さらに、コンテンツデータの受信に際して、受信コンテンツに対応するコピー履歴テーブルを受信し、受信したコピー履歴テーブルに基づくコピー制御処理を実行する構成を有することを特徴とする。

【0017】さらに、本発明の第2の側面は、コンテンツデータを格納したコンテンツ格納記録媒体からコンテンツデータを他の情報処理装置または他の記録媒体に出力可能な情報処理装置における情報処理方法であり、前記コンテンツ格納記録媒体に格納されたコンテンツデータについての、前記他の情報処理装置または他の記録媒体に対するコピー可否判定処理を、前記コンテンツデータ毎のコピー可能回数を設定したコピー履歴テーブルに基づいて判定することを特徴とする情報処理方法にある。

【0018】さらに、本発明の情報処理方法の一実施態

様において、前記コピー履歴テーブルには、コピー可能回数に対応して設定されるコピー番号と、コピー番号毎に対応して設定されるコピー格納先メディアID設定欄を有し、前記コピー可否判定処理は、コンテンツデータのコピー先となる他の情報処理装置または他の記録媒体の識別子を前記コピー格納先メディアID欄に記録可能か否かを判定するステップと、前記コピー格納先メディアID欄に記録可能であることを条件として前記コンテンツ格納記録媒体からのコピーを可能と判定するステップと、を含むことを特徴とする。

【0019】さらに、本発明の情報処理方法の一実施態様において、前記コンテンツ格納記録媒体の識別子と、前記情報処理装置に格納されたマスターキーとに基づいて、暗号化キーを生成し、前記暗号化キーに基づいて前記コピー履歴テーブルを暗号化して前記コンテンツ格納記録媒体、または該コンテンツ格納記録媒体を装着した情報処理装置内のメモリに格納する処理を実行することを特徴とする。

【0020】さらに、本発明の情報処理方法の一実施態様において、前記コピー履歴テーブルには、コピー可能回数に対応して設定されるコピー番号と、コピー番号毎に対応して設定されるコピー格納先メディアID設定欄を有し、前記コピー可否判定処理は、コンテンツデータのコピー先となる他の情報処理装置または他の記録媒体の識別子と同一の識別子が既に前記コピー格納先メディアID欄に記録されている場合には、同一の識別子を有する他の情報処理装置または他の記録媒体に対する前記コンテンツ格納記録媒体からのコピーを実行可と判定することを特徴とする。

【0021】さらに、本発明の情報処理方法の一実施態様において、コピーの可否を設定したコピー制御情報に基づいて、前記コンテンツデータを格納したコンテンツ格納記録媒体からのコンテンツデータのコピーの可否を判定するステップを有し、前記コピー制御情報には、コピーの可否とともに、コピーの許容回数が設定されていることを示す態様としての、コピー数制限ありを示す情報を含み、前記コピー制御情報がコピー数制限ありを示す情報であるか否かを判定し、コピー数制限ありを示すコピー制御情報であると判定されたことを条件として、前記他の情報処理装置または他の記録媒体に対するコピー可否判定処理を、前記コンテンツデータ毎のコピー可能回数を設定したコピー履歴テーブルに基づいて実行することを特徴とする。

【0022】さらに、本発明の情報処理方法の一実施態様において、コンテンツデータの受信に際して、コピーの可否を設定したコピー制御情報を受信し、コピー制御情報が、コピーの許容回数が設定されていることを示す態様としてのコピー数制限ありを示す情報である場合に、前記コピー履歴テーブルを生成して、生成したコピー履歴テーブルに基づくコピー制御処理を実行すること

を特徴とする。

【0023】さらに、本発明の情報処理方法の一実施態様において、コンテンツデータの受信に際して、コピーの可否を設定したコピー制御情報を受信し、コピー制御情報が、コピーの許容回数が設定されていることを示す態様としてのコピー数制限ありを示す情報であり、さらにコピーの許容回数の指定データが前記コピー制御情報中に含まれる場合に、前記コピー履歴テーブルを、前記コピー制御情報中のコピーの許容回数データに基づいて生成して、生成したコピー履歴テーブルに基づくコピー制御処理を実行することを特徴とする。

【0024】さらに、本発明の情報処理方法の一実施態様において、コンテンツデータの受信に際して、コピーの可否を設定したコピー制御情報を受信し、コピー制御情報が、コピーの許容回数が設定されていることを示す態様としてのコピー数制限ありを示す情報であり、コピーの許容回数の指定データが前記コピー制御情報中に含まれない場合に、前記コピー履歴テーブルを、前記情報処理装置に予め設定済みのコピー許容回数データに基づいて生成して、生成したコピー履歴テーブルに基づくコピー制御処理を実行することを特徴とする。

【0025】さらに、本発明の情報処理方法の一実施態様において、コンテンツデータの受信に際して、受信コンテンツに対応するコピー履歴テーブルを受信し、受信したコピー履歴テーブルに基づくコピー制御処理を実行することを特徴とする。

【0026】さらに、本発明の第3の側面は、コンテンツデータを格納した情報記録媒体であり、前記記録媒体に格納されたコンテンツデータについて、コンテンツデータ毎のコピー可能回数を設定したコピー履歴テーブルを格納したことを特徴とする情報記録媒体にある。

【0027】さらに、本発明の情報記録媒体の一実施態様において、前記コピー履歴テーブルには、コピー可能回数に対応して設定されるコピー番号と、コピー番号毎に対応して設定されるコピー格納先メディアID設定欄を有することを特徴とする。

【0028】さらに、本発明の情報記録媒体の一実施態様において、前記コピー履歴テーブルは、前記コンテンツ格納記録媒体の識別子と、前記情報処理装置に格納されたマスターキーとに基づいて生成される暗号化キーで暗号化されて格納された構成であることを特徴とする。

【0029】さらに、本発明の情報記録媒体の一実施態様において、前記コピー履歴テーブルには、複数のコンテンツデータの各々に対応して許容可能な個別のコピー可能回数が設定された構成であることを特徴とする。

【0030】さらに、本発明の第4の側面は、コンテンツ格納記録媒体に格納されたコンテンツデータについての、他の情報処理装置または他の記録媒体に対するコピー可否判定処理をコンピュータ・システム上で実行せしめるコンピュータ・プログラムを提供するプログラム提

供媒体であって、前記コンピュータ・プログラムは、コンテンツデータのコピー先となる他の情報処理装置または他の記録媒体の識別子を前記コピー格納先メディア I D 欄に記録可能か否かを判定するステップと、前記コピー格納先メディア I D 欄に記録可能であることを条件として前記コンテンツ格納記録媒体からのコピーが可能であると判定するステップと、を有することを特徴とするプログラム提供媒体にある。

【0031】なお、本発明の第4の側面に係るプログラム提供媒体は、例えば、様々なプログラム・コードを実行可能な汎用コンピュータ・システムに対して、コンピュータ・プログラムをコンピュータ可読な形式で提供する媒体である。媒体は、CDやFD、MOなどの記録媒体、あるいは、ネットワークなどの伝送媒体など、その形態は特に限定されない。

【0032】このようなプログラム提供媒体は、コンピュータ・システム上で所定のコンピュータ・プログラムの機能を実現するための、コンピュータ・プログラムと提供媒体との構造上又は機能上の協働関係を定義したものである。換言すれば、該提供媒体を介してコンピュータ・プログラムをコンピュータ・システムにインストールすることによって、コンピュータ・システム上では協働的作用が発揮され、本発明の他の側面と同様の作用効果を得ることができるのである。

【0033】本発明のさらに他の目的、特徴や利点は、後述する本発明の実施例や添付する図面に基づくより詳細な説明によって明らかになるであろう。

【0034】

【発明の実施の形態】【実施例1】図1は、本発明を適用した情報処理装置としての記録再生装置100の一実施例形態の構成を示すブロック図である。記録再生装置100は、入出力 I/F (Interface) 120、MPEG (Moving Picture Experts Group) コーデック130、A/D、D/Aコンバータ141を備えた入出力 I/F (Interface) 140、暗号処理手段150、CPU (Central Processing Unit) 170、メモリ180、記録媒体195に対する記録媒体インタフェース (I/F) 190を有し、これらはバス110によって相互に接続されている。

【0035】入出力 I/F 120は、外部から供給される画像、音声、プログラム等の各種コンテンツを構成するデジタル信号を受信し、バス110上に出力するとともに、バス110上のデジタル信号を受信し、外部に出力する。MPEGコーデック130は、バス110を介して供給されるMPEG符号化されたデータを、MPEGデコードし、入出力 I/F 140に出力するとともに、入出力 I/F 140から供給されるデジタル信号をMPEGエンコードしてバス110上に出力する。入出力 I/F 140は、A/D、D/Aコンバータ141を内蔵している。入出力 I/F 140は、外部から供

給されるコンテンツとしてのアナログ信号を受信し、A/D、D/Aコンバータ141でA/D (Analog Digital) 変換することで、デジタル信号として、MPEGコーデック130に出力するとともに、MPEGコーデック130からのデジタル信号を、A/D、D/Aコンバータ141でD/A (Digital Analog) 変換することで、アナログ信号として、外部に出力する。

【0036】暗号処理手段150は、例えば、1チップのLSI (Large Scale Integrated Circuit) で構成され、バス110を介して供給されるコンテンツとしてのデジタル信号を暗号化し、または復号し、バス110上に出力する構成を持つ。なお、暗号処理手段150は1チップLSIに限らず、各種のソフトウェアまたはハードウェアを組み合わせた構成によって実現することも可能である。ソフトウェア構成による処理手段としての構成については後段で説明する。

【0037】CPU 170は、メモリ180に記憶されたプログラムを実行することで、MPEGコーデック130や暗号処理手段150等を制御する。さらに、後段で詳細に説明するが本発明に特有のコピー履歴テーブルの読み出し処理、さらにコピー履歴テーブルを参照したコピー実行の可否判定処理等の制御手段の主要構成要素として機能する。メモリ180は、例えば、不揮発性メモリで、CPU 170が実行するプログラムや、CPU 170の動作に必要なデータを記憶する。例えば、後段で詳細に説明するコピー実行の可否判定処理プログラムを格納する。記録媒体インタフェース190は、デジタルデータを記録再生可能な記録媒体195を駆動することにより、記録媒体195からデジタルデータを読み出し (再生し)、バス110上に出力するとともに、バス110を介して供給されるデジタルデータを、記録媒体195に供給して記録させる。

【0038】記録媒体195は、例えば、DVD、CD等の光ディスク、光磁気ディスク、磁気ディスク、磁気テープ、あるいはRAM等の半導体メモリ等のデジタルデータの記憶可能な媒体であり、本実施の形態では、記録媒体インタフェース190対して着脱可能な構成であるとする。但し、記録媒体195は、記録再生装置100に内蔵する構成としてもよい。

【0039】なお、記録媒体195には個々の記録媒体を識別するための媒体識別情報 (メディアID) が記録されている。具体的には、本出願人による先の特許出願、特開平11-224461号公報 (特願平10-25310号) において説明しているが、個々の記録媒体を識別する為の媒体識別情報を、他のデータとともに記録媒体に記録し、この媒体識別情報のライセンスを受けた装置であることを条件として、その条件が満たされた場合にのみ記録媒体の媒体識別情報へのアクセスが可能となる。

【0040】この方法では、記録媒体上のデータは、媒

体識別情報とライセンスを受けることにより得られる秘密キー（マスターキー）により暗号化され、ライセンスを受けていない装置が、この暗号化されたデータを読み出したとしても、意味のあるデータを得ることができないようになっている。例えば前述のデバイスキーを用いて復号キーを生成する構成として、ライセンスを受けたデバイスに復号キーを生成可能なデバイスキーを付与する構成とする。なお、装置はライセンスを受ける際、不正な複製（違法コピー）ができないように、その動作が規定される。

【0041】ライセンスを受けていない装置は、媒体識別情報にアクセスできず、また、媒体識別情報は個々の媒体毎に個別の値となっているため、ライセンスを受けていない装置が、記録媒体に記録されている、暗号化されたデータのすべてを新たな記録媒体に複製したとしても、そのようにして作成された記録媒体に記録されたデータは、ライセンスを受けていない装置は勿論、ライセンスを受けた装置においても、正しく復号することができないから、実質的に、違法コピーが防止されることになる。

【0042】なお、本発明の記録再生装置の構成例としては図1に示す構成の他に図2に示す構成が可能である。図2に示す記録再生装置200では、記録媒体195はドライブ装置としての記録媒体インタフェース（I/F）190とともに記録再生装置200に内蔵されており、外部から入力されるデータ書き込みは、内蔵された記録媒体195に対して実行される。

【0043】図3に、本発明を利用した機器を用いたデータのコピーを行う場合の機器構成の一例を示す。図3においては、図1に示した記録再生機器を2台用いて、これら2台の機器をデジタルバス300を用いて接続し、記録媒体（メディア1）に記録されているコンテンツデータを記録媒体（メディア2）にコピーする様子を示している。

【0044】記録媒体（メディア1）にはあらかじめ、1つあるいは複数のコンテンツデータが記録され、それぞれのコンテンツデータについて、そのデータを元（親）として作成してよいコピー（子）の個数が決められている。この個数は、システムで一意に設定してもよいし、コンテンツデータごとに個別に設定してもよい。

【0045】さらに、記録媒体（メディア1）には、図4に示すコピー履歴テーブルが格納される。このテーブルは、たとえばその記録媒体に格納されているデータが、始めてコピーされる際に記録再生機器により生成される構成としてもよいし、記録媒体（メディア1）にコンテンツデータが記録される際に記録再生機器により作られるようにしてもよい。

【0046】コピー履歴テーブルには、コンテンツデータの識別情報であるコンテンツID、そのデータから作られたコピー（子）の番号、コピーの格納先の記録媒体

の識別情報であるメディアIDが格納される。

【0047】たとえば図4に示したコピー履歴のテーブルの例では、この記録媒体にはコンテンツID：12345678とabcd1234というコンテンツデータが記録されており、コンテンツID=12345678のデータは、コピー番号の欄が1～Nまで設定されており、N個までコピーを作ることが許されている。図4の例では、コンテンツID=12345678のデータは、コピー格納先メディアIDの欄に記録されているように、既に記録媒体識別番号（メディアID）がabcdefghと87654321という識別情報を持つ記録媒体にコピーが行われている。このテーブルを持つ記録媒体に格納されたコンテンツのコピーが実行されると、テーブルの対応コンテンツIDのコピー格納先メディアID欄にコピー番号1からNまで、順次、コピーデータの格納先となるメディアIDが記録される。図4の例では、コピー番号：3以降のコピーはまだ作られていないため、コピー番号3からNについては空欄となっている。同様にコンテンツID=abcd1234のコンテンツは、M個までコピーを作ることが許されており、識別番号87654321の記録媒体に1つコピーが行われたことを意味している。

【0048】なお、後段で説明するが、記録媒体が記録再生装置に内蔵された構成である場合は、図4のコピー履歴テーブルのコピー格納先メディアID欄にコピー格納先記録再生装置（情報処理装置）の識別子を格納する構成としてもよい。また、コピー履歴テーブルを記録媒体自体に格納せず、記録再生装置内のメモリに格納する構成として、必要に応じて読み出す構成としてもよい。

【0049】本発明の情報処理装置は、記録媒体に格納されたコンテンツデータについて、他の情報処理装置または他の記録媒体に対するコピー可否判定処理を、上述したコンテンツデータ毎のコピー可能回数を設定したコピー履歴テーブルに基づいて判定する。この判定処理は、図1または図2の記録再生装置構成における制御手段によって実行される。具体的には、制御手段の構成要素はCPU170であり、メモリ180に格納された処理プログラムに従ってCPU170が処理を実行する。

【0050】図4に示すように、コピー履歴テーブルには、コピー可能回数に対応して設定されるコピー番号と、コピー番号毎に対応して設定されるコピー格納先メディアID設定欄を有し、制御手段としてのCPU170は、コンテンツデータのコピー先となる他の情報処理装置または他の記録媒体の識別子を前記コピー格納先メディアID欄に記録する処理を実行し、IDが新たに記録されたことを条件としてコンテンツ格納記録媒体からのコピーを実行する。

【0051】ただし、コンテンツデータのコピー先となる他の情報処理装置または他の記録媒体の識別子と同一の識別子が既に前記コピー格納先メディアID欄に記録されている場合には、同一の識別子を有する他の情報処

10

20

30

40

50

理装置または他の記録媒体に対するコンテンツ格納記録媒体からのコピーは繰り返し実行可能であり、新たな識別子を持つ他の情報処理装置または他の記録媒体に対するコピー時にのみ、そのIDをコピー履歴テーブルに記録する処理を実行する。

【0052】なお、本実施例では、記録媒体（メディア1）は、例えば図5に示すような中心孔501、RAM領域502を有するRAMメディアとすることが可能であり、この場合、コンテンツデータおよびコピー履歴テーブルはともにRAMメディア上に格納する。また、記録媒体（メディア1）は、図6に示すような中心孔601、RAM領域602、ROM領域603を有するRAMとROMの混在メディアとした構成も可能であり、この場合、コンテンツデータをROM領域603に格納し、コピー履歴テーブルをRAM領域602に格納するように構成してもよい。

【0053】また、記録媒体（メディア1）は、図7に示すような、カートリッジ701にROMまたはRAMからなる光ディスク702を収納し、さらに不揮発メモリを有するICチップ703を持つ構成、すなわち、ROMメディアと書き換え可能な記憶領域を持つICチップが組み合わさった記録媒体とすることも可能であり、この場合、例えばコンテンツデータは光ディスク702のROM領域に、コピー履歴テーブルをICチップ703にそれぞれ格納する。さらに、記録媒体（メディア1）は、図8に示すような記録可能な領域を持つ1つもしくは複数のICチップ804を有するカートリッジ801とすることも可能である。カートリッジ801には、記録再生機器接続用の入出力端子802、メモリコントロール用ICチップ803を有する。このカートリッジ801においては、コンテンツデータ、コピー履歴テーブルともにICチップ804に格納される。

【0054】図9に、図3の構成を用いて記録再生機器A（デバイスA）に接続された記録媒体（メディア1）上のコンテンツデータを記録再生機器B（デバイスB）に接続された記録媒体（メディア2）にコピーする場合の処理フローを示す。一連の処理は、たとえば、記録再生機器B（デバイスB）から記録再生機器A（デバイスA）に対してあるコンテンツデータのコピーを要求するコマンドを送信することによって開始される。

【0055】図9のステップS901において、記録再生機器A（デバイスA）と記録再生機器B（デバイスB）はお互いの正当性を確認するために、相互認証および鍵共有プロトコルを実行し、このプロトコルを用いて共有した暗号鍵をそれ以降の通信に用いる。ただし、システムが高度のセキュリティを必要としない場合には、このプロトコルを行わなくてもよい。

【0056】相互認証のプロトコルの例としては、ISO/IEC 9798-2に代表される、共通鍵暗号を用いるもの、ISO/IEC 9798-3に代表される、公開鍵暗号を用いるもの

の、ISO/IEC 9798-4に代表される、暗号学的チェック関数を用いるものなどが挙げられる。

【0057】図10は、暗号学的チェック関数を用いた相互認証および暗号鍵共有のための方法のひとつを本実施例に用いたものである。図10において、記録再生機器A（デバイスA）と記録再生機器B（デバイスB）は、システム共通の秘密鍵：DKを、たとえばメモリ180に格納している。まず、デバイスBは乱数R_Bを発生し、デバイスAに送る。

【0058】次にデバイスAは、乱数R_A、S_Aを生成し、R_A、S_AとともにMAC(DK, R_A || R_B || S_A)をデバイスBに送る。MAC(DK, R_A || R_B || S_A)は、暗号学的チェック関数に鍵としてシステム共通の秘密鍵：DKを、データとしてR_A || R_B || S_Aを入力することを表す。暗号学的チェック関数は、ISO/IEC 9797に示されているように、FIPS 46-2のデータ暗号化規格（Data Encryption Standard, DES）を用いて構成することが可能である。なお、図10における記号||は連結を表している。

【0059】デバイスBは、受信したデータを用いて自分でもMAC(DK, R_A || R_B || S_A)を計算し、これが受信したものと一致するかを検査する。一致すれば、デバイスAが正当なものであるとして認め、処理を続けるが、一致しなければデバイスBが不正なものであると判断して処理を中止する。

【0060】次にデバイスBは乱数S_Bを生成し、これとMAC(DK, R_B || R_A || S_B)をデバイスAに送る。

【0061】デバイスAも受信したデータを用いて自分でMAC(DK, R_B || R_A || S_B)を計算し、受信したものと一致するかを確認する。一致すれば、デバイスBが正当なものであるとして認め、処理を続けるが、一致しなければデバイスBが不正なものと判断して処理を中止する。

【0062】最後に、双方がMAC(DK, S_A || S_B)を計算し、これをそのセッションにおけるセッションキーとして使用する。

【0063】上記のようにすることにより、2つの記録再生装置は互いの正当性を検査することができ、またセッションキーを安全に共有することができたので、例えば、このセッションキーを鍵として、そのセッションの通信内容を暗号化することにより安全に相手に送信することが可能となる。

【0064】図11は、公開鍵暗号、具体的には楕円曲線暗号を用いた認証技術を本実施例に適用したものである。

【0065】図11において、デバイスAおよびデバイスBは、それぞれ自分の識別情報であるIDと、自分の公開鍵証明書、およびリボケーションリストまたはレジストレーションリストを持っている。公開鍵証明書は、

図12に示すように、そのエンティティのIDと、公開鍵に対し、信頼できるセンタがデジタル署名を施したデータである。

【0066】リボケーションリストは、不正者リストあるいはブラックリストとも呼ばれ、図13に示すように、その装置の秘密鍵が露呈してしまったもののIDがリストアップされ、単調に増加するバージョンナンバーとともにセンタのデジタル署名が施されたものである。

【0067】これに対し、レジストレーションリストは、正当者リストあるいは登録リストとも呼ばれ、図14に示すように、その時点で信頼できる（秘密が露呈していない）装置のIDがリストアップされ、単調に増加するバージョンナンバーとともにセンタのデジタル署名が施されたものである。

【0068】図11において、デバイスBは乱数 R_B を発生させ、デバイスAに送る。デバイスAは、乱数 K_A および R_A を発生させ、楕円曲線E上でシステム共通の点（ベースポイント）であるGと K_A を乗算して V_A を計算し、さらに自分の秘密鍵（PriKey_A）を用いてデータ $R_A || R_B || V_A$ に対して施した署名ととともに、公開鍵証明書（Cert_A）と $R_A || R_B || V_A$ をデバイスBに送る。

【0069】デバイスBは、デバイスAの公開鍵証明書の正当性、デバイスAが作成した署名の正当性を検査する。そして、自分がリボケーションリストを格納していれば、相手のIDがリボケーションリストに載っていないことを、また、自分がレジストレーションリストを格納していれば、相手のIDがレジストレーションリストに登録されていることを確認する。以上の確認が正常にできなければ、デバイスBはデバイスAが不正者であると判断して処理を終了する。以上の確認が正常にできれば、デバイスBは、乱数 K_B を生成して、デバイスAが行ったのと同様な計算を行い、公開鍵証明書（Cert_B）と R_B, R_A, V_B とともにデータ $R_B || R_A || V_B$ に対して施した署名をデバイスAに送る。

【0070】デバイスAでは、上記のデバイスBが行ったのと同様の検査を受信したデータに対して行い、すべての検査が正常に終了したときのみ処理を継続する。

【0071】この後、デバイスAでは K_A と V_B を、デバイスBでは K_B と V_A を、それぞれ楕円曲線E上で乗算してセッションキー K_S を得る。セッションキーの使用法については、上述の暗号学的チェック関数を用いた相互認証の場合と同様である。

【0072】なお、楕円曲線上の乗算やデジタル署名の生成および検査方法については、現在IEEE P1363で規格制定中であり、そのドラフトに詳細が記されている。

【0073】図9に戻り、図3の構成において、記録再生機器A（デバイスA）に接続された記録媒体（メディア1）上のコンテンツデータを記録再生機器B（デバイスB）に接続された記録媒体（メディア2）にコピーする場

合の処理フローの説明を続ける。ステップS902において、デバイスBはデバイスAに、記録媒体（メディア2）の識別情報（メディアID）を送信する。

【0074】ステップS903において、デバイスAは、記録媒体（メディア1）からコピー履歴テーブルを読み出し、そのコンテンツデータをデバイスBに接続された記録媒体（メディア2）にコピーしてよいか否かを判断する。

【0075】この判断は、基本的には、コピー履歴テーブルの、そのコンテンツに対応するコピー先メディアIDの欄に空欄があるかどうか、すなわち、既に許容個数までコピーが作成されていないかどうかを用いて判断される。空欄があれば、コピーが許され、空欄がなければコピーは許可されない。

【0076】また、すでにそのコンテンツデータのコピーが行われ、コピー履歴テーブルにそのIDが記録されている記録媒体に対して行われるコピーについては、コピー（子）の個数を増やさないと決めることも可能である。即ち、たとえば図4のコピー履歴テーブルにおいてコンテンツID 12345678のデータのコピー格納先メディアIDの欄がN個すべて埋まっていた場合、基本的にはこのデータからの新たなコピーは許可されないが、コピー格納先メディアIDに記されたメディアIDを持つ記録媒体に対するコピーのみは許可されるとするものである。ステップS903の詳細を図15の処理フローを用いて説明する。

【0077】図15は、本出願と同一の出願人に係る先の特許出願である特開平11-224461号公報で提案した方式、すなわち複数の記録再生機器に共通に格納された秘密鍵（マスターキー）と記録媒体固有情報から暗号化キーおよび復号キーを生成する手法に、本発明のコピー制御情報によるコピー制御処理を適用した場合の処理、すなわち記録媒体に格納したコピー履歴テーブル（図4参照）の暗号化、復号処理に秘密鍵（マスターキー）と記録媒体固有情報（メディアID）とから生成した鍵を用いる処理フローである。

【0078】ステップS1501において、コピー履歴テーブルを格納した記録媒体をアクセスしたデバイス（図3の例では、記録再生機器A（デバイスA））はメディア1のメディアIDを読み出す。

【0079】次に、デバイスAは、ステップS1502において、メディア1のメディアIDと自身が格納しているマスターキーに基づいて暗号鍵を生成する。さらに、ステップS1503で、デバイスはメディア1から暗号化されて格納されているコピー履歴テーブルを読み出す。ステップS1504において、デバイスAはステップS1502で生成した暗号鍵を用いてコピー履歴テーブルを復号する。さらに、ステップS1505において、デバイスAは上述した手順に従ってコピーの許可、不許可を判定する。すなわち、先に図4を用いて説明し

たコピー履歴テーブルにおいて、コピー対象のコンテンツIDのデータに対応して設定されたコピー番号の欄1〜Xに対応するコピー格納先メディアIDの欄に空欄がある場合にのみ、コピー可と判断する。

【0080】図9に戻り、処理フローの説明を続ける。ステップS903において、コピーが許可されない場合には、ステップS904乃至S906をスキップし、コピーを行わずに処理を終了する。一方、コピーが許可される場合にはステップS904に進む。

【0081】ステップS904において、デバイスAはコピー履歴テーブルを変更する必要があるかどうかを判定する。基本的には、コピーを行う場合にはコピー先のメディアIDを新たにテーブルに書き加える必要があるため、テーブルの変更が必要である。ただし、上述のように、同じメディアIDを持つ記録媒体へのコピーは何回行っても1回と考えるというルールの下では、今回のコピー先のメディアIDが既にテーブルのそのコンテンツデータに対応するコピー先メディアIDの欄に記録されている場合には、コピー履歴テーブルの変更は必要ではない。

【0082】テーブルの変更が必要でない場合にはステップS905をスキップしてステップS906に進み、テーブルの変更が必要であればステップS905に進む。

【0083】ステップS905では、デバイスAはコピー履歴テーブルの変更を行う。具体的には、そのコンテンツデータに対応するコピー先メディアIDの空いている欄に今回コピーを作る記録媒体のメディアIDを追記する。ステップS905の詳細を図16の処理フローを用いて説明する。

【0084】図16は、特開平11-224461号公報で提案した方式、すなわち複数の記録再生機器に共通に格納された秘密鍵（マスターキー）と記録媒体固有情報から暗号化キーおよび復号キーを生成する手法を本発明のコピー履歴テーブルの変更（編集）処理に応用した場合の処理フローである。

【0085】デバイスAがメディア1上のコピー履歴テーブルを変更（編集）する処理において、図16のステップS1601乃至S1604は、図15のステップS1501乃至S1504と同一であり、記録再生機器に共通に格納された秘密鍵（マスターキー）と記録媒体固有情報としてのメディアIDから復号キーを生成してコピー履歴テーブルを復号するステップである。

【0086】ステップS1605において、実際にコピー履歴テーブルを編集する。ここでの編集は、先に図4を用いて説明したように、コピー対象となるコンテンツIDに対応して設定されたコピー格納先メディアID欄に、新たにコピーを実行するメディアのメディアIDを書き込む処理である。コピー履歴テーブルの編集が終了すると、ステップS1606において、先に生成したデ

ータ暗号鍵を用いて編集後のコピー履歴テーブルを暗号化し、ステップS1607において暗号化したコピー履歴テーブルをメディア1に記録する。

【0087】図9に戻り、処理フローの説明を続ける。上述のような処理に従ったコピー履歴テーブルの編集処理が終了すると、ステップS906に進む。ステップS906では、デバイスAおよびデバイスBの両機器はコンテンツデータのコピーを実行する。

【0088】次に、図17に、デバイスAのメディア1からデバイスBのメディア2に対するコンテンツデータのコピー処理において、デバイスAおよびデバイスBの各々において実行される処理を簡潔に説明したフローを示す。以下、図17の各処理ステップについて説明する。

【0089】図17も前述の図15、16と同様、本出願と同一の出願人に係る先の特許出願である特開平11-224461号公報で提案した方式、すなわち複数の記録再生機器に共通に格納された秘密鍵（マスターキー）と記録媒体固有情報から暗号化キーおよび復号キーを生成する手法と、本発明のコピー制御情報によるコピー制御処理とを併せて実行した場合の処理フローである。また、図17に示す処理フローは、デバイスAがメディア1上のコピー履歴テーブルを用いてコピーの許可／不許可を判断し、コピー可である場合、すなわち、先に図4を用いて説明したコピー履歴テーブルにおいて、コピー対象のコンテンツIDのデータに対応して設定されたコピー番号の欄1〜Xに対応して設定されたコピー格納先メディアIDの欄に空欄があり、コピー可と判断された場合に実行されるフローである。

【0090】図17の処理フローの左側はデバイスAの処理、右側はデバイスBの処理である。ステップS1701およびステップS1721において、デバイスAおよびデバイスBは、例えば先に図10、11を用いて説明した処理に従って、相互認証処理およびセッションキー生成処理を実行する。相互認証が成立し、セッションキーの生成に成功すると次のステップに進む。認証がエラーとなった場合は以下の処理は実行されない。

【0091】ステップS1702において、デバイスAはメディア1のメディアIDを読み出し、ステップS1722において、デバイスBはメディア2のメディアIDを読み出す。デバイスBはステップS1723において、読み出したメディア2のメディアIDをデバイスAに送信する。この際、送信メディアIDはセッションキーで暗号化して送信してもよい。

【0092】デバイスAは、ステップS1703において、メディア1のメディアIDと自身が格納しているマスターキーに基づいて、メディア1上のデータを暗号化する暗号鍵（これを暗号鍵(1)と呼ぶ）を生成する。さらに、ステップS1704で、デバイスAはメディア1からコピー履歴テーブルおよびコピー対象となるコンテ

ンツデータを読み出す。

【0093】ステップS1705において、デバイスAはメディア1からコピーすべきコンテンツデータと、コピー履歴テーブルとを先に生成した暗号鍵(暗号鍵(1))を用いて復号する。

【0094】ステップS1706において、デバイスAは、ステップS1723でデバイスBから、受信したメディア2のメディアIDに基づいてコピー履歴テーブルの更新処理を実行する。具体的には、先に図4を用いて説明したように、コピー対象となるコンテンツIDに対応して設定されたコピー格納先メディアID欄に、新たにコピーを実行するメディアのメディアIDを書き込む。

【0095】ステップS1707において、デバイスAはステップS1701でデバイスBと共有したセッションキーを用いてコンテンツデータを暗号化し、ステップS1708で暗号化コンテンツデータをデバイスBに送信する。なお、コンテンツデータを暗号化して伝送する方法として、××××××××××××××××××××××××5社によって定められている、5CDTCP(Five Company Digital Transmission Content Protection)(以下、適宜、DTCPという)を用いてもよい。ここで、DTCPについては、例えば、<http://www.dtcp.com>のURL(Uniform Resource Locator)で特定されるWebページにおいて、インフォメショナルバージョン(Informational Version)の仕様書の取得が可能である。

【0096】さらに、ステップS1709において、デバイスAは、先に生成したデータ暗号鍵(暗号鍵(1))を用いて編集後のコピー履歴テーブルを暗号化し、ステップS1710において暗号化したコピー履歴テーブルをメディア1に記録する。

【0097】ステップS1724において、デバイスBは暗号化されたコンテンツデータを受信する。ステップS1725において、デバイスBはステップS1721で共有したセッションキーを用いて受信した暗号化コンテンツデータを復号する。

【0098】次に、ステップS1726において、デバイスBはメディア2から読み出したメディアIDと、自身が格納するマスターキーを用いてデータを暗号化する暗号鍵(暗号鍵(2)と呼ぶ)を生成する。ステップS1727において、デバイスBは暗号鍵(2)を用いてコンテンツデータを暗号化し、ステップS1728において暗号化データをメディア2に記録する。

【0099】以上の処理により、メディア1のコンテンツデータについて、許容された個数の範囲内の個数のコピーとなるようなコピーをメディア2に作成することができる。ステップS1706において、コピー履歴テーブルの更新処理、すなわち、コピー対象となるコンテンツIDに対応して設定されたコピー格納先メディアID欄に、新たにコピーを実行するメディアのメディアID

を書き込む処理が実行できない場合、すなわち、予めコピー履歴テーブルのコピー番号として設定された数を超える場合は、メディアIDを書き込めないことになり、以下の処理ステップS1707以下の処理が実行されない。この場合は、デバイスBに対するコピー処理が実行されない。

【0100】なお、上記の例では、コピー先の記録媒体(メディア2)が図1に示すようなリムーバブルメディアであることを前提としているが、これが図2の記録媒体のような、記録再生装置と一体型となっている記録媒体の場合、即ち、図18に示す構成となっている場合には、メディア2のメディアIDの代わりに、コピー先の記録再生装置(デバイスB)の識別情報(デバイスID)を使用することも可能である。この場合、コピー履歴テーブルのコピー先メディアIDの欄にはデバイスIDを記録してもよい。

【0101】さらに、コピー先の記録媒体が記録再生装置と一体型となっている場合のみならず、リムーバブル型の記録媒体の場合であっても、記録媒体のメディアIDの代わりに記録再生装置のデバイスIDを使用することは可能である。記録媒体上のデータが、それを記録した記録再生装置でのみ再生できるような暗号化をされる仕組みになっている場合に最も効果が大いだが、そうでない場合でも実施可能である。

【0102】また、上記の例では、コピー履歴テーブルを、記録媒体(メディア1)上に格納するようにしているが、これをコピー元の記録再生装置(デバイスA)内のたとえばメモリ180に格納するようにしてもよい。これも記録媒体上のデータが、それを記録した記録再生装置でのみ再生できるような暗号化をされる仕組みになっている場合に最も効果が大いだが、そうでない場合でも実施可能である。また、このようにすることにより、コピー元の記録媒体(メディア1)が書き込み可能な領域を持たない場合にも対応可能となる。

【0103】[実施例2] 図19は、本発明を適用した記録再生装置の別の実施の形態の構成例を示している。図19に示す記録再生装置1900は、図1に示すものとはほぼ同様であるが、2つの記録媒体I/F1901、および1902を持ち、それぞれが記録媒体1951および1952と接続されるようになっている。

【0104】図20に、図19に示した記録再生装置を用いたコピーの処理フローを示す。この構成においては、実施例1で説明した図9のステップS901のような機器間での相互認証プロトコルは不要となっている。

【0105】ステップS2001において、記録再生装置はコピー先となるメディア2のメディアIDを読み出し、ステップS2002では、コピーしてよいか否かの判断を行う。コピーの可否の判断は、先に図4を用いて説明したように、コピー履歴テーブル、この場合は、メディア1に格納されたコピー履歴テーブルにおいて、コ

ビー対象のコンテンツIDのデータに対応して設定されたコピー番号の欄1〜Xに対応するコピー格納先メディアIDの欄に空欄がある場合にコピー可と判断する。

【0106】ステップS2003およびS2004は、図9のステップS904およびS905と同様であるので説明を省略する。

【0107】ステップS2005では、メディア1からメディア2に対するコンテンツのコピーを実行する。このコンテンツコピー処理の詳細を図21のフローに示す。

【0108】図21の処理フローは、先に述べた他の処理フローと同様、特開平11-224461号公報で提案した方式、すなわち複数の記録再生機器に共通に格納された秘密鍵（マスターキー）と記録媒体固有情報から暗号化キーおよび復号キーを生成する手法を適用した場合の処理フローである。

【0109】図21のステップS2101乃至S2104は、先に説明した図17のデバイスAでの処理ステップS1702、S1703と、デバイスBでの処理ステップS1722、S1723に相当するものであり、本実施例においては、同一機器内において、メディア1、2のIDを読み出して、それぞれのメディア用の暗号鍵（1）、（2）を生成する。

【0110】ステップS2105では、メディア1からコピーすべきコンテンツデータと、コピー履歴テーブルを読み出して、ステップS2106において、先のステップS2102で生成した暗号鍵（暗号鍵（1））を用いて、コンテンツデータと、コピー履歴テーブルとの復号処理を実行する。

【0111】ステップS2107において、デバイスAは、復号したコピー履歴テーブルの編集処理を実行する。具体的には、図4に示すコピー履歴テーブルのコピー対象となるコンテンツのコピー格納先メディアID欄にメディア2のIDを書き込む。この書き込み処理の後、先に生成したデータ暗号鍵（暗号鍵（1））を用いて編集後のコピー履歴テーブルを暗号化し、暗号化したコピー履歴テーブルをメディア1に記録する。

【0112】次に、ステップS2108において、デバイスAは暗号鍵（2）を用いてコンテンツデータを暗号化し、ステップS2109において暗号化データをメディア2に記録する。

【0113】実施例2の構成では、図20、21の処理フローから理解されるように、図17において2つの記録再生装置が行っていた処理を1つの記録再生装置が行うようになっているため、装置間でコンテンツデータを伝送する処理を省略できる。

【0114】【実施例3】以上の説明においては、コピー履歴テーブルの編集更新処理を行なうことにより、コピーの数を制限する構成について説明したが、従来例の欄で説明したSCMS (Serial Copy Management System)

m)と組み合わせて、ネットワーク配信によるコンテンツ配信においてもコピーの数を制限することを可能とした構成について実施例3として説明する。これまでに規定されているSCMSには、何度でもコピーが許容されるコピーフリー (copy free) のデータであるか、1度だけコピーが許されている (copy once allowed) データであるか、またはコピーが禁止されている (copy prohibited) データであるか、これら3態様を表す信号が含まれる。上記3つの態様に加え、さらにコピー履歴テーブルによるコピー数を制限する場合を、コピー数制限ありとして設定する。このような設定をすることにより、インターネットを介したコンテンツ配信のようなネットワーク配信において、コンテンツプロバイダからの一次配信を受信した機器からの2次配信回数を制限することが可能となる。

【0115】例えばSCMS信号として2ビット設定し、コピーフリー (copy free) の場合、[0, 0]、1度だけコピーが許されている (copy once allowed) を [0, 1]、コピー禁止 (copy prohibited) を [1, 1] とし、コピー履歴テーブルによるコピー数制限ありの場合を、[1, 1] とする。これら4態様をSCMS信号として設定してコピーの制限を行なう。SCMS信号が [1, 1]、すなわち、コピー履歴テーブルによるコピー数制限ありの場合には、コピー数を設定するビットとしてコピー数設定ビットを数ビット、例えば4ビットを設定し、許可されたコピー数に応じて、コピー数設定ビットを設定する。例えば3回のみコピー可であれば [0011]、5回コピー可であれば、[0101] 等である。コンテンツプロバイダは、コンテンツの配信先にコンテンツとともに、これらのコピー数設定ビットを送信する。

【0116】コンテンツプロバイダからの一次配信を受信する機器において、コピー履歴テーブルによるコピー数制限ありの [1, 1] の信号およびコピー数設定ビットを受信した場合、予め機器に格納されている、あるいは配信されるコピー履歴テーブル生成処理プログラムに従って、コピー数設定ビットに設定されたコピー数に応じたコピー履歴テーブルを生成する。生成したコピー履歴テーブルは、受信コンテンツとともに記録媒体に格納される。

【0117】生成するコピー履歴テーブルは、先に説明した図4と同様のものとなるが、コンテンツに対応して設定されるコピー番号は、コピー数設定ビットに設定された数、例えば、[0011] であれば3、[0101] であれば5を上限とした数に設定される。なお、SCMS信号が [1, 1] であり、コピー数設定ビットにコピー数の指定がない場合、もしくはコピー数設定ビットが伝送されない場合には、システムにあらかじめ定められているコピー数に対応したテーブルが作られる。すなわち、情報処理装置に予め設定済みのコピー許容回数

データ、例えばコピー数設定ビットの付与されないコンテンツに共通に適用するデータとして情報処理装置に設定されているコピー許容回数データに基づいてコピー履歴テーブルを生成して、生成したコピー制御テーブルに基づいてコピー制御処理を実行する。

【0118】このように、コピー制限数をコンテンツと併せて配信することにより、記録媒体から再生されてコピーされるコンテンツのみでなく、ネットワークを介して配信されるコンテンツに対してもコピー数の制限を行なうことが可能となる。

【0119】なお、コピー数設定ビットに基づいてコピー履歴テーブルを生成する構成に限らず、例えばコンテンツとともに、予め所定のコピー番号が設定されたコピー履歴テーブルを、コンテンツプロバイダが送信する構成としてもよい。また、予め所定のコピー番号が設定されたテーブル生成コマンドを送信して、受信側においてコマンドに応じたコピー履歴テーブルを生成する構成としてもよい。

【0120】〔データ処理手段の構成〕上述した一連の処理は、ハードウェアにより行うことは勿論、ソフトウェアにより行うこともできる。即ち、例えば、図1他で示す記録再生装置に構成される暗号処理手段150は暗号化/復号LSIとして構成することも可能であるが、汎用のコンピュータや、1チップのマイクロコンピュータにプログラムを実行させることにより行う構成とすることも可能である。一連の処理をソフトウェアによって行う場合には、そのソフトウェアを構成するプログラムが、汎用のコンピュータや1チップのマイクロコンピュータ等にインストールされる。図22は、上述した一連の処理を実行するプログラムがインストールされるコン

ピュータの一実施の形態の構成例を示している。

【0121】プログラムは、コンピュータに内蔵されている記録媒体としてのハードディスク2205やROM2203に予め記録しておくことができる。あるいは、プログラムはフロッピー（登録商標）ディスク、CD-ROM(Compact Disc Read Only Memory)、MO(Magneto optical)ディスク、DVD(Digital Versatile Disc)、磁気ディスク、半導体メモリなどのリムーバブル記録媒体2210に、一時的あるいは永続的に格納（記録）しておくことができる。このようなリムーバブル記録媒体2210は、いわゆるパッケージソフトウェアとして提供することができる。

【0122】なお、プログラムは、上述したようなリムーバブル記録媒体2210からコンピュータにインストールする他、ダウンロードサイトから、デジタル衛星放送用の人工衛星を介して、コンピュータに無線で転送したり、LAN(Local Area Network)、インターネットといったネットワークを介して、コンピュータに有線で転送し、コンピュータでは、そのようにして転送されてくるプログラムを、通信部2208で受信し、内蔵する

ハードディスク2205にインストールすることができる。

【0123】コンピュータは、CPU(Central Processing Unit)2202を内蔵している。CPU2202には、バス2201を介して、入出力インタフェース2211が接続されており、CPU2202は、入出力インタフェース2210を介して、ユーザによって、キーボードやマウス等で構成される入力部2207が操作されることにより指令が入力されると、それにしたがって、ROM(Read Only Memory)2203に格納されているプログラムを実行する。

【0124】あるいは、CPU2202は、ハードディスク2205に格納されているプログラム、衛星若しくはネットワークから転送され、通信部2208で受信されてハードディスク2205にインストールされたプログラム、またはドライブ2209に装着されたリムーバブル記録媒体2210から読み出されてハードディスク2205にインストールされたプログラムを、RAM(Random Access Memory)2204にロードして実行する。

【0125】これにより、CPU2202は、上述したフローチャートにしたがった処理、あるいは上述したブロック図の構成により行われる処理を行う。そして、CPU2202は、その処理結果を、必要に応じて、例えば、入出力インタフェース2211を介して、LCD(Liquid Crystal Display)やスピーカ等で構成される出力部2206から出力、あるいは、通信部2208から送信、さらには、ハードディスク2205に記録させる。

【0126】ここで、本明細書において、コンピュータに各種の処理を行わせるためのプログラムを記述する処理ステップは、必ずしもフローチャートとして記載された順序に沿って時系列に処理する必要はなく、並列的あるいは個別に実行される処理（例えば、並列処理あるいはオブジェクトによる処理）も含むものである。

【0127】また、プログラムは、1つのコンピュータにより処理されるものであっても良いし、複数のコンピュータによって分散処理されるものであっても良い。さらに、プログラムは、遠方のコンピュータに転送されて実行されるものであっても良い。

【0128】なお、暗号化/復号処理は、1チップの暗号化/復号LSIで実行する構成、あるいはCPUが実行する1つのソフトウェアモジュールとして実現することも可能である。

【0129】以上、特定の実施例を参照しながら、本発明について詳解してきた。しかしながら、本発明の要旨を逸脱しない範囲で当業者が該実施例の修正や代用を成し得ることは自明である。すなわち、例示という形態で本発明を開示してきたのであり、限定的に解釈されるべきではない。本発明の要旨を判断するためには、冒頭に記載した特許請求の範囲の欄を参照すべきである。

【0130】

【発明の効果】以上、説明したように、本発明の情報処理装置では、コピー数を設定したコピー履歴テーブルをコンテンツに対応付けて保有する構成としたので、データ（コンテンツ）ごとに作られるコピー（子）の数の制限が可能となる。具体的には、コンテンツデータごとにコピーの履歴テーブルを作成し、それに基づいてコピーを行うかどうか判定し、上限に達した以降のコピー処理を不可とする。すなわち、コピー実行の前に、コンテンツIDに対応して設定されたコピー格納先メディアID欄に、コピーを実行するメディアのメディアIDを書き込む処理を実行する構成としたので、予めコピー履歴テーブルのコピー番号として設定された数を超える場合は、メディアIDを書き込まず、コピーが実行されない。従って、テーブルに設定したコピーの数を越えるコピーが氾濫することを防止できる。

【0131】さらに、本発明の情報処理装置では、コピー制限数をコンテンツと併せて配信することにより、記録媒体から再生されてコピーされるコンテンツのみでなく、ネットワークを介して配信されるコンテンツに対してもコピー数の制限を行なうことが可能となる。

【図面の簡単な説明】

【図1】本発明の情報処理装置の構成例1を示すブロック図である。

【図2】本発明の情報処理装置の構成例2を示すブロック図である。

【図3】本発明の情報処理装置のコンテンツコピー時の接続態様例を示すブロック図である。

【図4】本発明の情報処理装置におけるコピー履歴テーブルの例を示す図である。

【図5】本発明の情報処理装置において使用可能な記録媒体の構成例（例1）を示す図である。

【図6】本発明の情報処理装置において使用可能な記録媒体の構成例（例2）を示す図である。

【図7】本発明の情報処理装置において使用可能な記録媒体の構成例（例3）を示す図である。

【図8】本発明の情報処理装置において使用可能な記録媒体の構成例（例4）を示す図である。

【図9】本発明の情報処理装置におけるコンテンツコピー処理フローを示す図である。

【図10】本発明の情報処理装置において適用可能な認証処理（共通鍵方式）の処理シーケンスを示す図である。

【図11】本発明の情報処理装置において適用可能な認証処理（公開鍵方式）の処理シーケンスを示す図である。

【図12】本発明の情報処理装置において適用可能な認証処理に用いられる公開鍵証明書の構成を示す図である。

【図13】本発明の情報処理装置におけるリボケーションリストの構成を示す図である。

【図14】本発明の情報処理装置におけるレジストレーションリストの構成を示す図である。

【図15】本発明の情報処理装置におけるコピー履歴テーブルを用いたコピー許可／不許可判定処理フローを示す図である。

【図16】本発明の情報処理装置におけるコピー履歴テーブルの編集処理、格納処理フローを示す図である。

【図17】本発明の情報処理装置におけるデバイス間でのコピー履歴テーブルを用いたコンテンツコピー処理フローを示す図である。

【図18】本発明の情報処理装置のコンテンツコピー時の接続態様例を示すブロック図である。

【図19】本発明の情報処理装置の実施例2における構成例を示すブロック図である。

【図20】本発明の情報処理装置の実施例2におけるコンテンツコピー処理フローを示す図である。

【図21】本発明の情報処理装置の実施例2におけるコンテンツコピー処理の詳細フローを示す図である。

【図22】本発明の情報処理装置において、データ処理をソフトウェアによって実行する場合の処理手段構成を示したブロック図である。

【符号の説明】

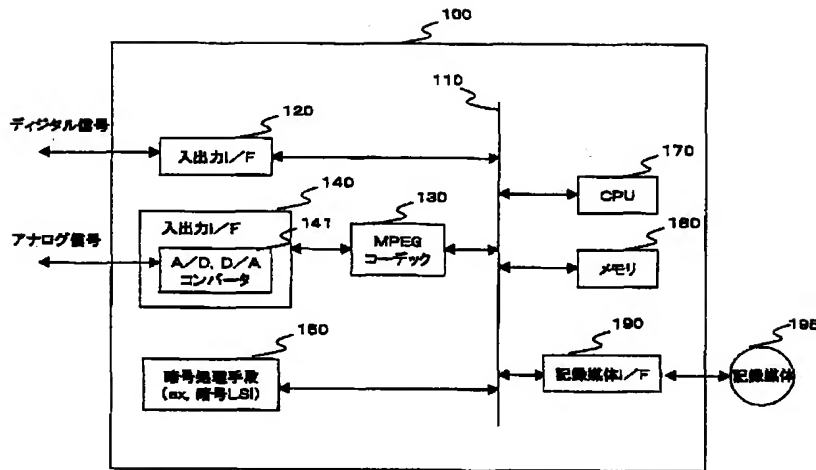
100, 200 記録再生装置
110 バス
120 デジタルI/F
130 MPEGコーデック
140 入出力I/F
145 A/D, D/Aコンバータ
150 暗号処理手段
170 CPU
180 メモリ
190 記録媒体I/F
195 記録媒体
501 中心孔
502 RAM領域
601 中心孔
602 RAM領域
603 ROM領域
701 カートリッジ
702 光ディスク
703 ICチップ
801 カートリッジ
802 入出力端子
803 メモリコントロール用ICチップ
804 ICチップ
1900 記録再生装置
1901, 1902 記録媒体I/F
1951, 1952 記録媒体
2201 バス
2202 CPU

2203 ROM
2204 RAM
2205 ハードディスク
2206 出力部
2207 入力部

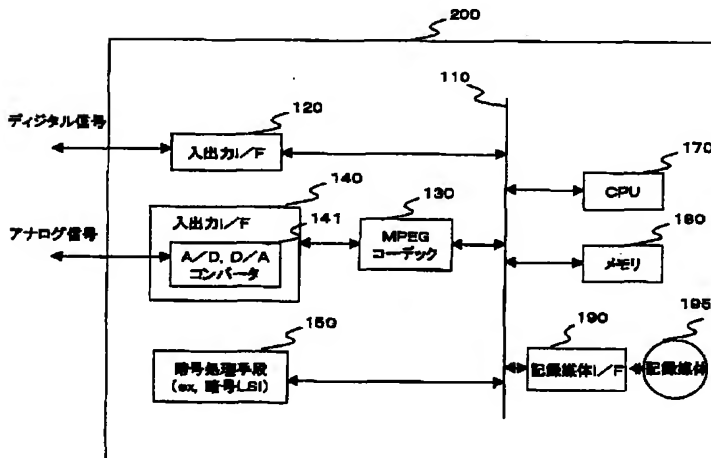
* 2208 通信部
2209 ドライブ
2210 リムーバブル記録媒体
2211 入出力インタフェース

*

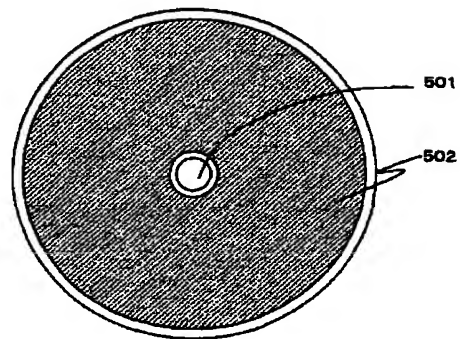
【図1】



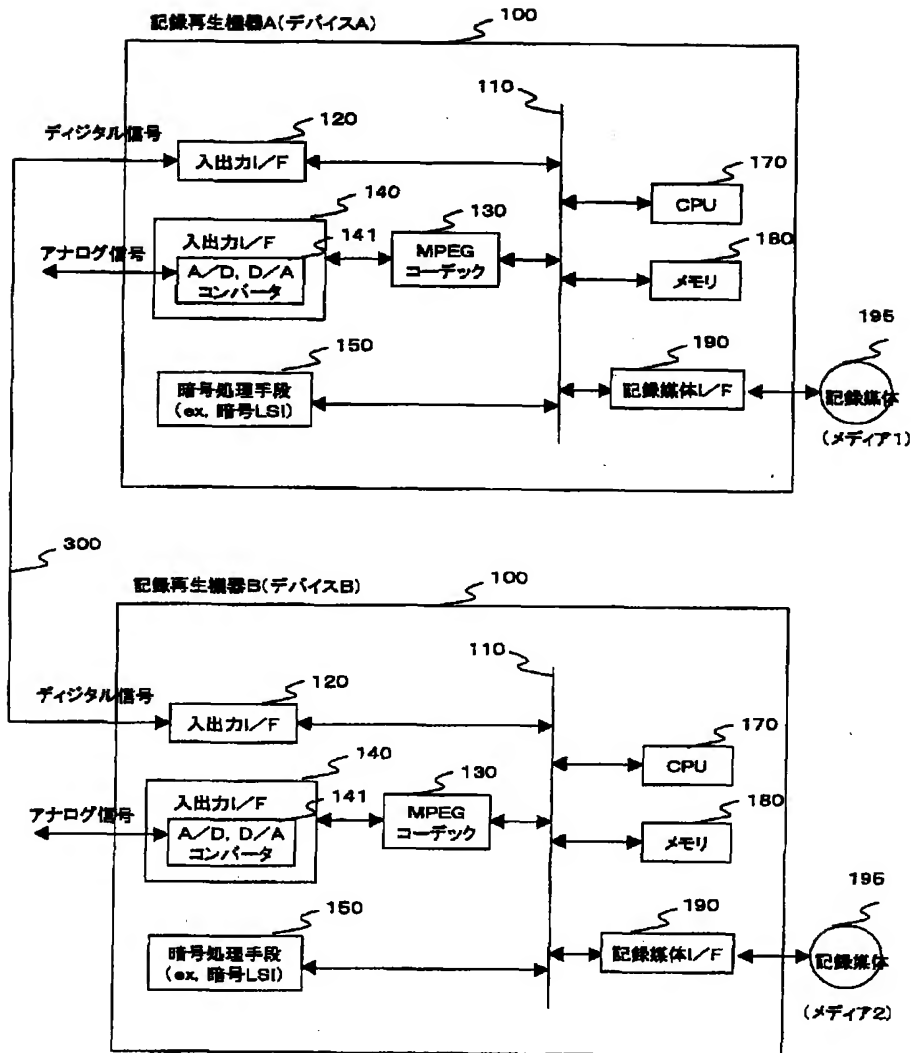
【図2】



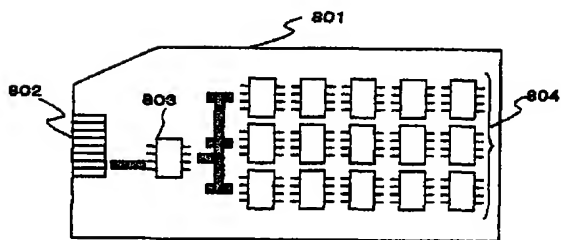
【図5】



【図3】



【図8】



【図13】

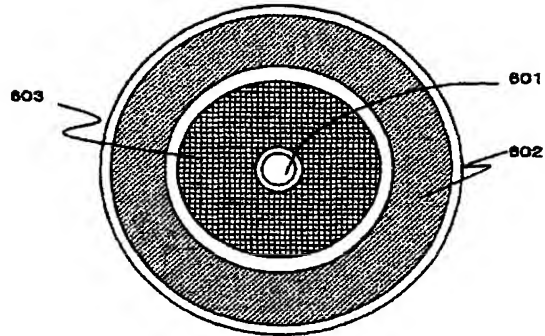
リポケーションリストのフォーマット

バージョンナンバ
リポークされる機器のID
:
センタのデジタル署名

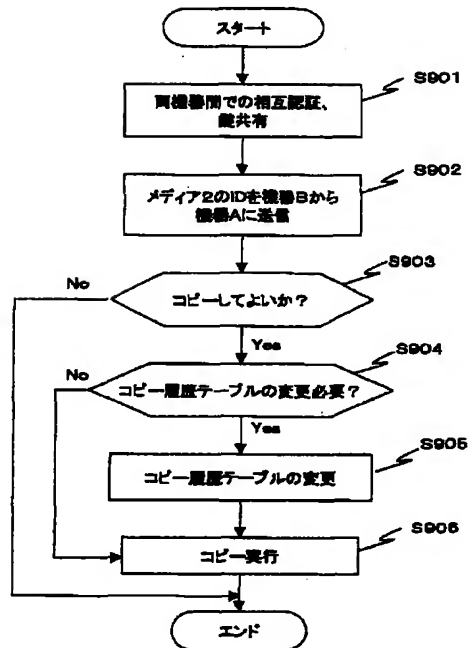
【図4】

コンテンツID	コピー番号	コピー格納先メディアID
12345678	1	abcdefgh
	2	87654321
	3	-----
	...	-----
	N	-----
abcd1234	1	87654321
	2	-----
	3	-----
	...	-----
	M	-----
:	:	:

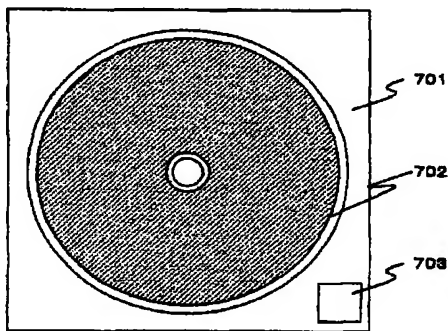
【図6】



【図9】



【図7】



【図12】

デバイスAの公開鍵証明書(Cert_A)

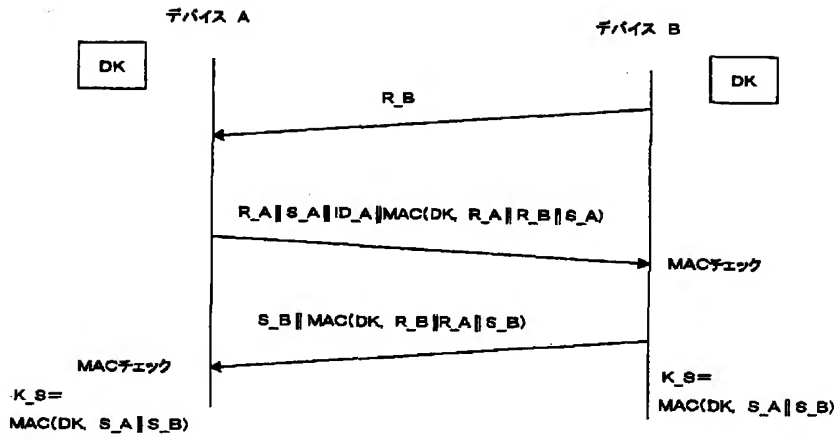
AのID(ID_A)
Aの公開鍵(Pubkey_A)
上記の全フィールドに対するセンタのデジタル署名

【図14】

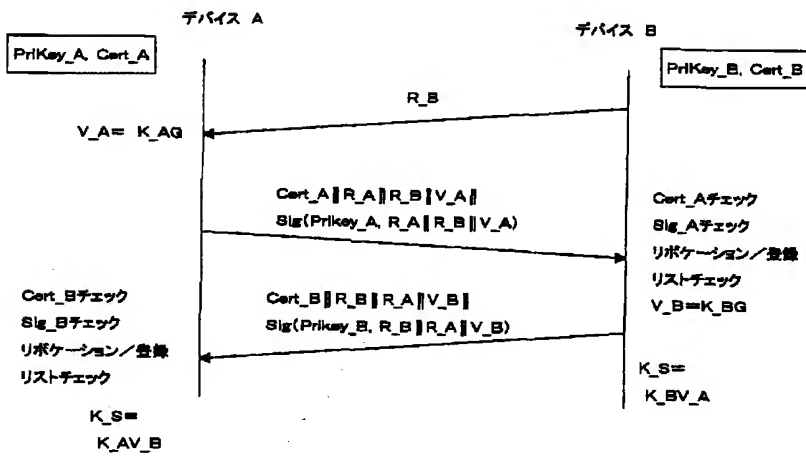
レジストレーションリストのフォーマット

バージョンナンバ
登録される機器のID
:
センタのデジタル署名

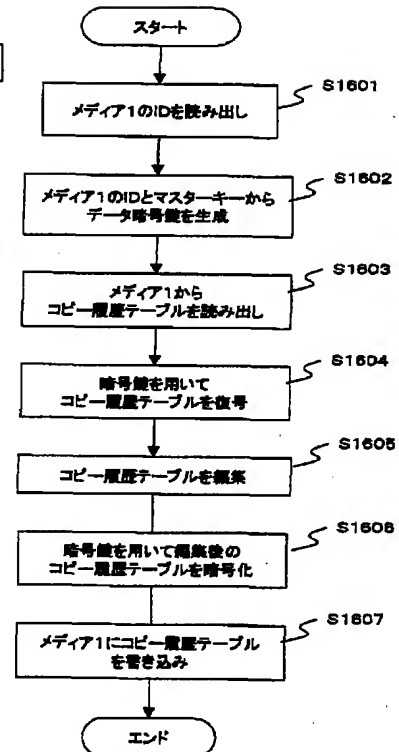
【図10】



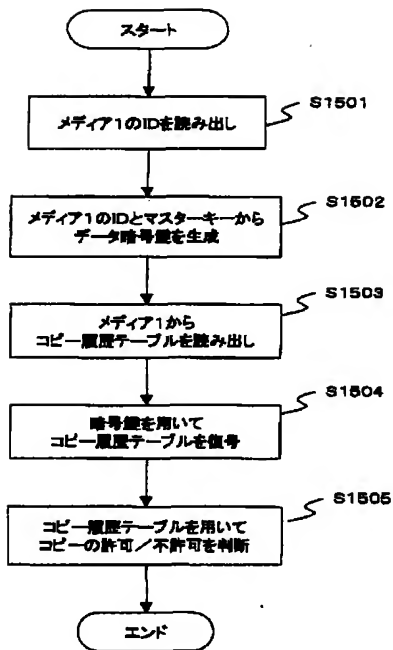
【図11】



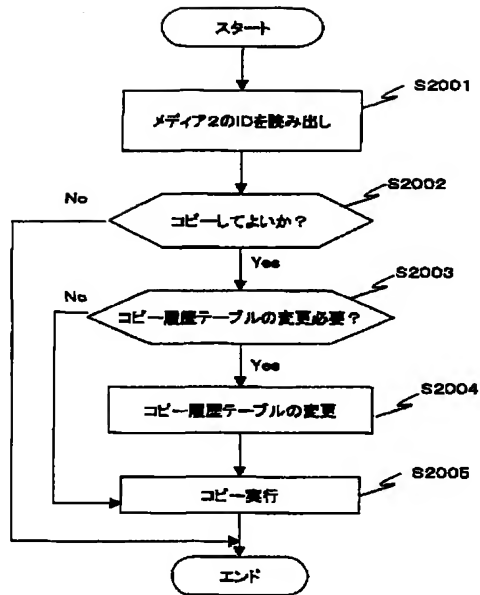
【図16】



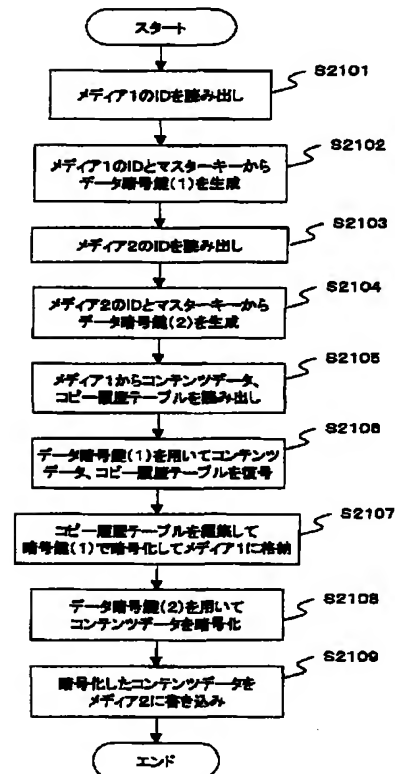
【図15】



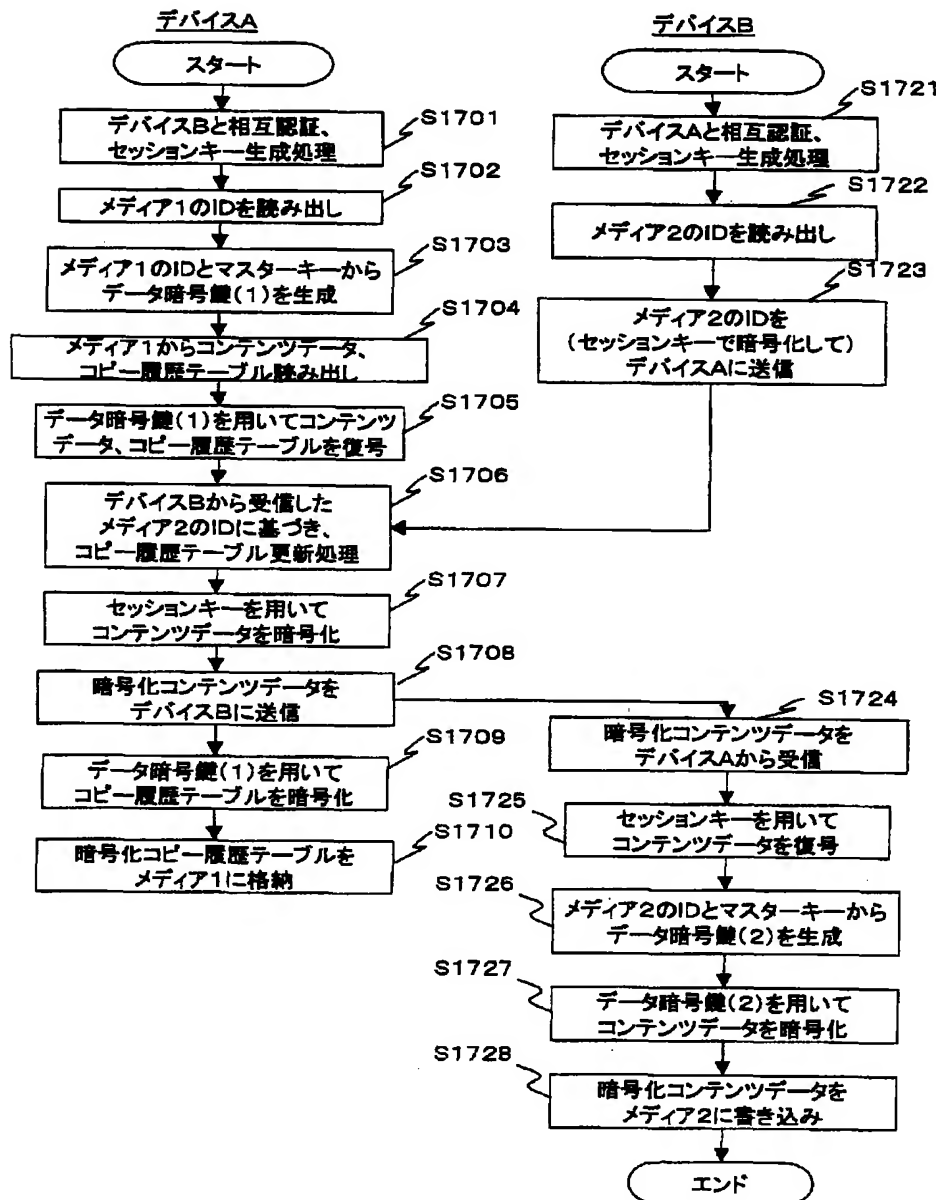
【図20】



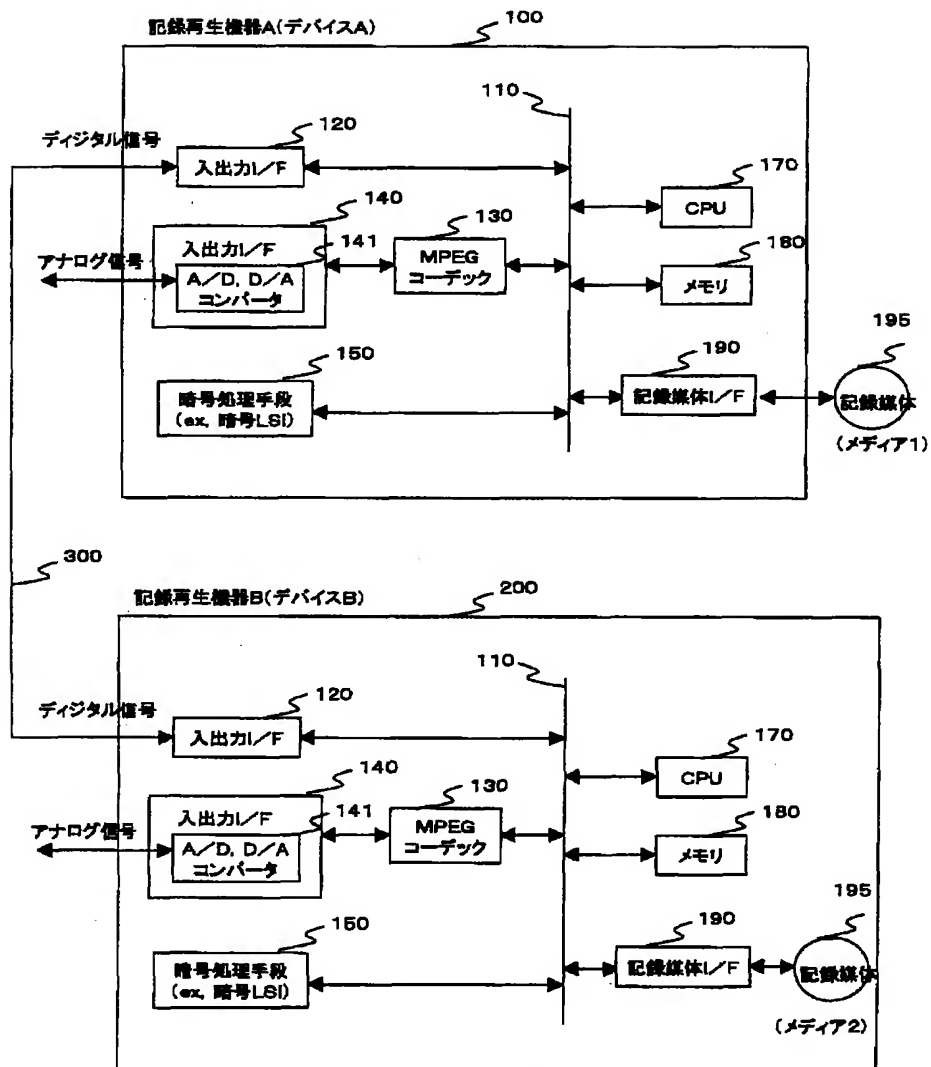
【図21】



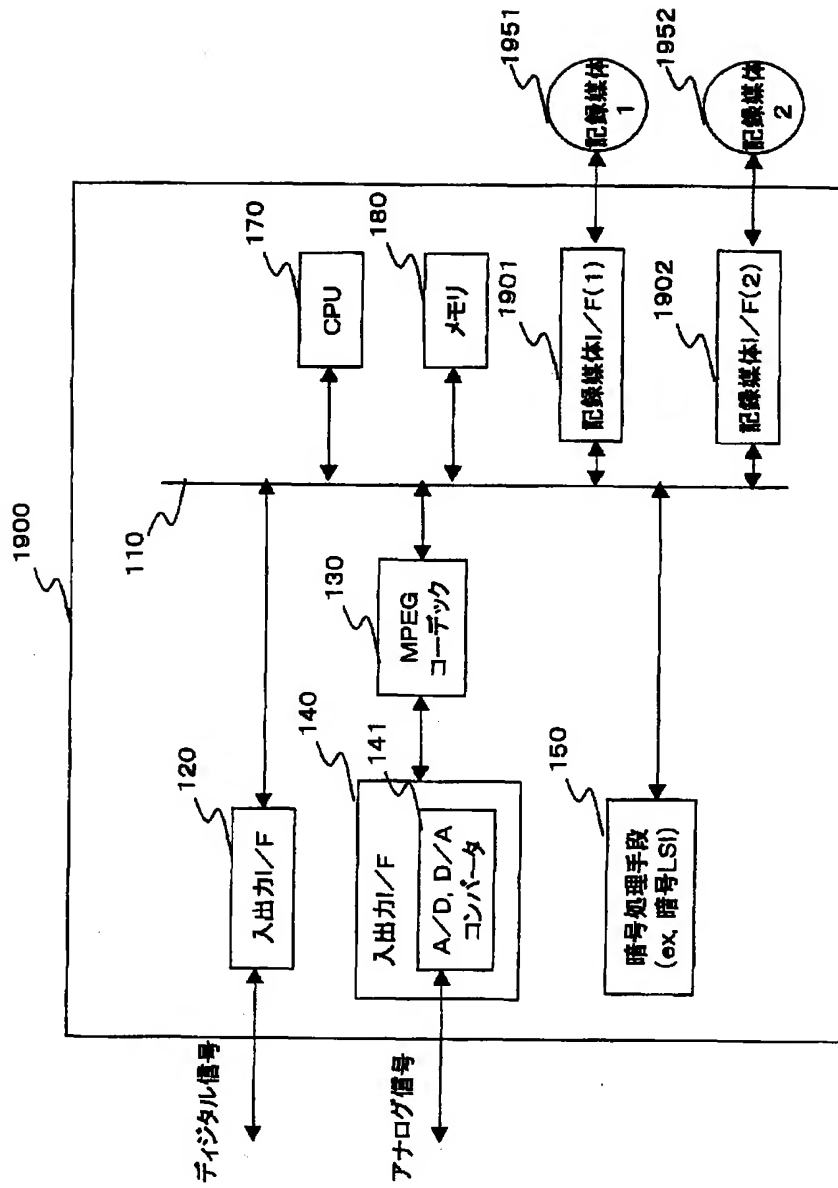
【図17】



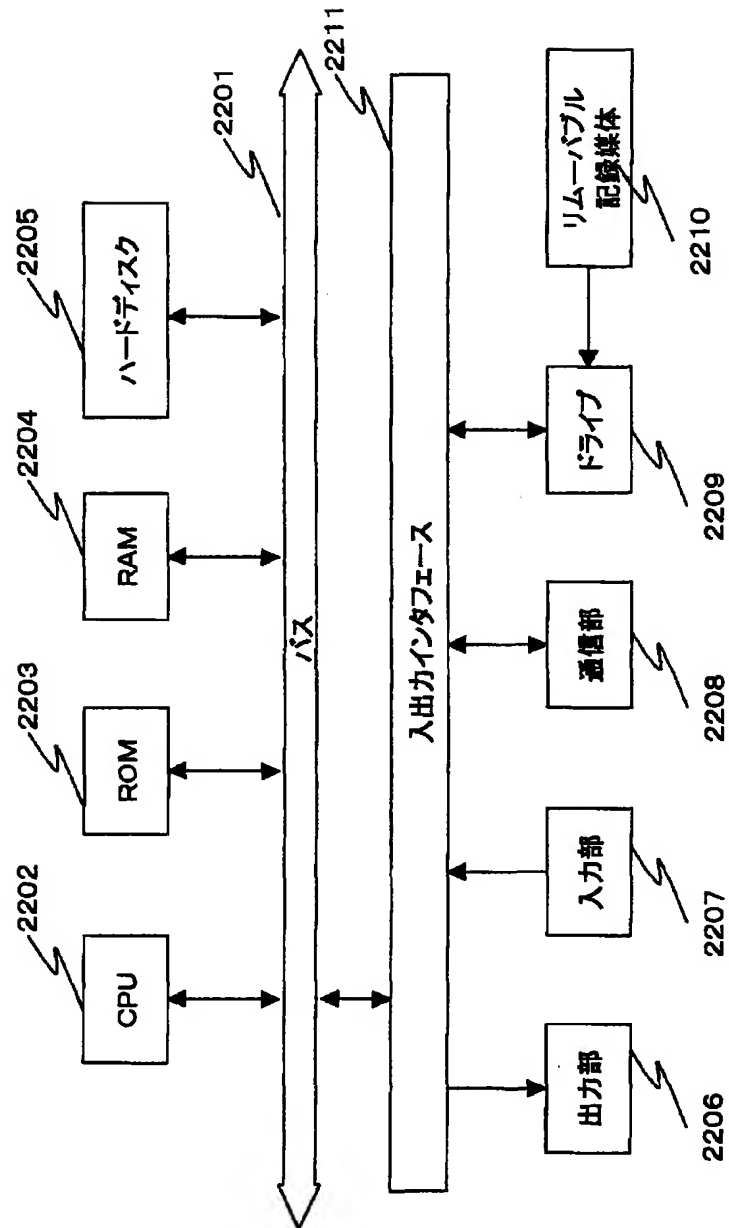
【図18】



【図19】



【図22】



フロントページの続き

(51)Int.Cl.⁷
G 0 6 F 17/60

識別記号
1 4 2

F I
G 0 6 F 17/60

テーマコード (参考)

1 4 2

(25)

特開 2001-351322

(72)発明者 中野 雄彦
東京都品川区北品川6丁目7番35号 ソニ
ー株式会社内
(72)発明者 北島 真理子
東京都品川区北品川6丁目7番35号 ソニ
ー株式会社内

F ターム(参考) 5B017 AA06 BA07 BB10 CA15 CA16
5B049 AA05 BB00 CC00 DD05 FF09
GG04
5D044 AB05 BC04 CC04 DE17 DE50
GK17 HL08